

# AUDIT REPORT

Hostname: Access\_SW3  
Config file name: access-sw3.txt  
Config hash: 17321b09cf96d20cf62fdf0dac157ff4df7be58c  
Vendor: cisco  
OS: ios  
Facility layer: access  
L3 protocols: ipv4,ipv6  
Enabled functions: acl created  
Date: 18/05/2020\_09:49

## SUCCESS STATISTICS

Weighted score coefficient: 88 out of 100

Successful checks: 84.0%

Unsuccessful checks: 16.0%

Total number of relevant started checks: 175

Successful checks: 144

Unsuccessful 'Critical': 12

Unsuccessful 'High': 4

Unsuccessful 'Medium': 11

Unsuccessful 'Low': 1

Unsuccessful 'Notice': 3

## Authentication, Authorization, Accounting

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	AAA new model/ Enabled AAA	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> aaa new-model					
2	AAA server set	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> radius server RADIUS_SERVER address ipv4 192.168.60.11 auth-port 1645 acct-port 1646 key RadKey1					
3	AAA server group	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> aaa group server radius RADIUS_SERVER server name RADIUS_SERVER					
4	AAA authentication login	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> aaa authentication login default group RADIUS_SERVER local enable					
5	AAA authentication login fallback	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> aaa authentication login default group RADIUS_SERVER local enable					

6	AAA authentication login only local disabled	High	False	False	Successful ✓
7	AAA authentication login none disabled	Critical	False	False	Successful ✓
8	AAA authentication "enable"	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> aaa authentication enable default group RADIUS_SERVER enable					
9	AAA authentication "enable" fallback	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> aaa authentication enable default group RADIUS_SERVER enable					
10	AAA authentication "enable" only local disabled	Medium	False	False	Successful ✓
11	AAA authentication "enable" none disabled	High	False	False	Successful ✓
12	AAA authorization "exec"	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> aaa authorization exec default group RADIUS_SERVER local if-authenticated					
13	AAA authorization "exec" fallback	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> aaa authorization exec default group RADIUS_SERVER local if-authenticated					
14	AAA authorization "exec" only local disabled	High	False	False	Successful ✓
15	AAA authorization "exec" none disabled	Critical	False	False	Successful ✓
16	AAA accounting "connection"	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> aaa accounting connection default start-stop group RADIUS_SERVER					
17	AAA accounting "connection" none disabled	High	False	False	Successful ✓
18	AAA accounting "exec"	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> aaa accounting exec default start-stop group RADIUS_SERVER					
19	AAA accounting "exec" none disabled	High	False	False	Successful ✓
20	AAA source interface	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> ip radius source-interface Loopback0					
21	AAA authentication max attempts less or equal to 5	High	False	False	Successful ✓

## Access to device

No.	Name	Severity	Skipped	Cannot determine Status search/fix	
1	Exec timeout <=5 minutes	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> line con 0 exec-timeout 5 0 line vty 0 4 exec-timeout 5 0					
2	AUX connection input disabled	High	False	False	Successful ✓
3	AUX no execution set	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> line aux 0 no exec					
4	Remote output connections disabled	Medium	False	False	Successful ✓

**Right configuration setting found in:**

line con 0  
transport output none  
line aux 0  
transport output none  
line vty 0 4  
transport output none

5	Local user database with encrypted password	Critical	False	False	Successful ✓
---	---------------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

username admin secret 5 \$1\$PPrf\$4VwGn/sDgGf9q4H1C8VMv0

6	Local user database with plaintext password disabled	Critical	False	False	Successful ✓
7	Enable password encrypted	Critical	False	False	Successful ✓

**Right configuration setting found in:**

enable secret 5 \$1\$fiHR\$A/2jfPoa67oq14z8lqC6H0

8	Enable password plaintext disabled	Critical	False	False	Successful ✓
9	Local login to virtual terminal disabled	Critical	False	False	Successful ✓
10	Restrict login to device - IPv4 ACL	Critical	False	False	Successful ✓

**Right configuration setting found in:**

line vty 0 4  
access-class IPV4\_VTY\_ACL in

11	ACL specified for VTY access is created	Critical	False	False	Error ✗
----	-----------------------------------------	----------	-------	-------	---------

**Comment:**

Cannot be fixed automatically!

**Fix notice:**

Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for managing devices with these commands:

ip access-list standard <acl name>  
remark Permitting managemnt device  
permit <ip address> <wildcard mask>

12	Log login to device on failure	High	False	False	Successful ✓
----	--------------------------------	------	-------	-------	--------------

**Right configuration setting found in:**

login on-failure log

13	Log login to device on success	Medium	False	False	Successful ✓
----	--------------------------------	--------	-------	-------	--------------

**Right configuration setting found in:**

login on-success log

14	Login quiet mode	Medium	False	False	Successful ✓
----	------------------	--------	-------	-------	--------------

**Right configuration setting found in:**

login quiet-mode access-class IPV4\_VTY\_ACL

15	ACL exists for specified login quiet mode	Medium	False	False	Error ✗
----	-------------------------------------------	--------	-------	-------	---------

**Comment:**

Cannot be fixed automatically!

**Fix notice:**

Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for managing devices with these commands:

ip access-list standard <acl name>  
remark Permitting managemnt device  
permit <ip address> <wildcard mask>

16	One user change config at time	High	False	False	Successful ✓
----	--------------------------------	------	-------	-------	--------------

**Right configuration setting found in:**

configuration mode exclusive

17	Legal banner MOTD	Low	False	False	Successful ✓
----	-------------------	-----	-------	-------	--------------

**Right configuration setting found in:**

banner motd ^C Unauthorized access will be prosecuted!! ^C

18	Legal banner exec	Low	False	False	Successful ✓
----	-------------------	-----	-------	-------	--------------

**Right configuration setting found in:**

banner exec ^C Unauthorized access will be prosecuted!! ^C

banner login ^C Unauthorized access will be prosecuted!! ^C

19	Legal banner login	Low	False	False	Successful ✓
----	--------------------	-----	-------	-------	--------------

**Right configuration setting found in:**

banner login ^C Unauthorized access will be prosecuted!! ^C

banner motd ^C Unauthorized access will be prosecuted!! ^C

20	Session timeout	Medium	False	False	Successful ✓
----	-----------------	--------	-------	-------	--------------

**Right configuration setting found in:**

line con 0

session-timeout 30

line aux 0

session-timeout 30

line vty 0 4

session-timeout 30

21	AUX exec timeout one second	High	False	False	Successful ✓
----	-----------------------------	------	-------	-------	--------------

**Right configuration setting found in:**

line aux 0

exec-timeout 0 1

22	Restrict login to device - IPv6 ACL	Critical	False	False	Successful ✓
----	-------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

line vty 0 4

ipv6 access-class IPV6\_VTY\_ACL in

23	ACL IPv6 specified for VTY access is created	Critical	False	False	Error ✗
----	----------------------------------------------	----------	-------	-------	---------

**Comment:**

Cannot be fixed automatically!

**Fix notice:**

Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for managing devices with these commands:

ipv6 access-list &lt;acl name&gt;

remark Permiting managemnt device

permit ip &lt;ip address&gt; &lt;wildcard mask&gt; any

24	Login DOS block for	High	False	False	Successful ✓
----	---------------------	------	-------	-------	--------------

**Right configuration setting found in:**

login block-for 120 attempts 3 within 30

## SSH

No.	Name	Severity	Skipped	Cannot determine Status search/fix
1	SSH enable on management connection	Critical	False	False Error ✗
<b>Found error in context(s):</b> line vty 0 4				
<b>Generated fix:</b> line vty 0 4 transport input ssh				
<b>Fix notice:</b> Make sure RSA key is present - generated or imported. For generating RSA key, issue command: crypto key generate rsa modulus 2048				
2	SSH version 2	Critical	False	False Error ✗
<b>Generated fix:</b> ip ssh version 2				
3	SSH timeout	Medium	False	False Error ✗

**Generated fix:**

ip ssh timeout 30  
ip ssh time-out 30

**Fix notice:**

Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

4	SSH max 3 retries	Medium	False	False	Successful ✓
5	SSH source interface	High	False	False	Error ✗

**Generated fix:**

ip ssh source-interface Loopback0

6	SSH not default port	High	False	False	Error ✗
---	----------------------	------	-------	-------	---------

**Generated fix:**

ip ssh port 2223 rotary 1

7	SSH not default port applied	High	False	False	Successful ✓
---	------------------------------	------	-------	-------	--------------

**Right configuration setting found in:**

line vty 0 4  
rotary 1

## Device identification

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Hostname set	Low	False	False	Successful ✓

**Comment:**

Cannot be fixed automatically!

**Right configuration setting found in:**

hostname Access\_SW3

2	Domain name set	Low	False	False	Successful ✓
---	-----------------	-----	-------	-------	--------------

**Right configuration setting found in:**

ip domain-name thesis-test.cz

3	All interfaces have description	Low	False	False	Error ✗
---	---------------------------------	-----	-------	-------	---------

**Comment:**

Cannot be fixed automatically!

**Found port(s) with error:**

Loopback0  
Ethernet0/0  
Ethernet0/1  
Ethernet0/2  
Ethernet0/3  
Ethernet1/0  
Ethernet1/1  
Ethernet1/2  
Ethernet1/3  
Ethernet2/0  
Ethernet2/1  
Ethernet2/2  
Ethernet2/3  
Ethernet3/0  
Ethernet3/1  
Ethernet3/2  
Ethernet3/3  
Serial4/0  
Serial4/1  
Serial4/2  
Serial4/3  
Serial5/0  
Serial5/1  
Serial5/2  
Serial5/3  
Vlan1

**Fix notice:**

Set interface description with command:  
 interface <interface name>  
 description <description of interface>

**Fix ignore comment:**

Fixing commands suppressed due to manual need of manual change and name determination.

## SNMP

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	SNMP v2 write disabled	Critical	False	False	Successful
2	SNMP v2 read without ACL disabled	Critical	False	False	Successful
3	SNMP v2 read with ACL disabled	Critical	False	False	Successful
4	SNMP v1 trap host disabled	Critical	False	False	Successful
5	SNMP v2 trap host disabled	Critical	False	False	Successful
6	SNMP v3 read [authnopriv noauth authpriv without ACL] or write disabled	Critical	False	False	Error
<b>Error configuration setting found in:</b> snmp-server group SNMP_V3_GRP v3 auth read READVIEWv3 access SNMP_V3 snmp-server group SNMP_V3_GRP_IPV6 v3 auth read READVIEWv3 access ipv6 SNMP_V3_ACL6					
7	SNMP v3 read authpriv with ACL enabled	Critical	False	False	Error
<b>Generated fix:</b> snmp-server group SNMP_V3_GRP v3 priv read READVIEWv3 access SNMP_V3 snmp-server user SNMPv3USER SNMP_V3_GRP v3 auth sha SnpPasswd123 priv aes 256 SnpPasswd123 access SNMP_V3					
8	SNMP v3 read authpriv with IPv6 ACL enabled	Critical	False	False	Error
<b>Generated fix:</b> snmp-server group SNMP_V3_GRP_IPV6 v3 priv read READVIEWv3 access ipv6 SNMP_V3_ACL6 snmp-server user SNMPv3USER SNMP_V3_GRP_IPV6 v3 auth sha SnpPasswd123 priv aes 256 SnpPasswd123 access SNMP_V3_ACL6					
9	SNMP user v1 v2c or v3 [noauth authnopriv no sha no aes without ACL] disabled	Critical	False	False	Successful
10	SNMP trap source interface	High	False	False	Successful
<b>Right configuration setting found in:</b> snmp-server trap-source Loopback0					
11	SNMP server location	High	False	False	Successful
<b>Right configuration setting found in:</b> snmp-server location GNS3LAB					
12	SNMP v3 traps priv	Medium	False	False	Error
<b>Generated fix:</b> snmp-server host 192.168.60.11 version 3 priv SNMPv3USER					
13	SNMP traps v3 read [authnopriv noauth] or v1 v2 disabled	Critical	False	False	Error
<b>Error configuration setting found in:</b> snmp-server host 192.168.60.11 version 3 auth SNMPv3USER					
14	SNMP traps enabled	Medium	False	False	Successful
<b>Right configuration setting found in:</b> snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart					
15	ACL is created for SNMPv3	Critical	False	False	Error

**Comment:**

Cannot be fixed automatically!

**Fix notice:**

Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for receiving SNMP with these commands:

ip access-list standard <acl name>

remark Permiting SNMP

permit <ip address> <wildcard mask>

16	ACL IPv6 is created for SNMPv3	Critical	False	False	Error ❌
----	--------------------------------	----------	-------	-------	---------

**Comment:**

Cannot be fixed automatically!

**Fix notice:**

Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for receiving SNMP with these commands:

ipv6 access-list <acl name>

remark Permiting managemnt device

permit ip <ip address> <wildcard mask> any

17	SNMP interface index persist enabled globally	High	False	False	Successful ✔
----	-----------------------------------------------	------	-------	-------	--------------

**Right configuration setting found in:**

snmp ifmib ifindex persist

18	SNMP interface index persist enabled per interface	High	False	False	Matched by equivalent ✔
----	----------------------------------------------------	------	-------	-------	-------------------------

**Comment:**

Module was marked as matched by equivalent by module 05\_20\_snmp\_ifindex\_persist\_globally.yaml

## Syslog

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Syslog server enabled	High	False	False	Successful ✔
<b>Right configuration setting found in:</b> logging host 192.168.60.11					
2	Syslog server IPv6 enabled	High	False	False	Not relevant ✔
<b>Comment:</b> Module 06_02_syslog_server_ipv6.yaml configured to run after 06_01_syslog_server.yaml with status error but that module has not run yet with specified cmd_match_status, 06_02_syslog_server_ipv6.yaml will not run					
3	Syslog source interface	Medium	False	False	Successful ✔
<b>Right configuration setting found in:</b> logging source-interface Loopback0					
4	Syslog format	Medium	False	False	Successful ✔
<b>Right configuration setting found in:</b> service timestamps log datetime msec					
5	Syslog critical alerts to console	Medium	False	False	Successful ✔
<b>Right configuration setting found in:</b> logging console critical					
6	Syslog send informational traps	High	False	False	Successful ✔
7	Syslog buffer set with severity	High	False	False	Successful ✔
<b>Right configuration setting found in:</b> logging buffered 40960 informational					
8	Syslog local backup	High	False	False	Successful ✔
<b>Right configuration setting found in:</b> logging persistent url unix:/					
9	Syslog sequence numbers added	Medium	False	False	Successful ✔

**Right configuration setting found in:**  
service sequence-numbers

## NTP

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	NTP server set	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> ntp server 192.168.60.11					
2	NTP source interface	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> ntp source Loopback0					
3	NTP authentication key	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> ntp authentication-key 1 md5 151C1F1C342B38373F37647040 7					
4	NTP trusted key	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> ntp trusted-key 1					
5	NTP authenticate	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> ntp authenticate					

## High load

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	SNMP traps for CPU load	Medium	False	False	Error ✗
<b>Generated fix:</b> snmp-server enable traps cpu threshold					
2	Threshold for CPU load	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> process cpu threshold type total rising 70 interval 5					
3	Statistics entry for CPU load	Low	False	False	Successful ✓
<b>Right configuration setting found in:</b> process cpu statistics limit entry-percentage 70					
4	Reserve memory for critical notification	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> memory reserve critical 1000					
5	Minimum CPU memory notification	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> memory free low-watermark processor 2000					
6	Minimum IO memory notification	Medium	False	False	Error ✗
<b>Generated fix:</b> memory free low-watermark io 2000					

## Spanning tree

No.	Name	Severity	Skipped	Cannot determine search/fix	Status



1	Portfast globally enabled	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> spanning-tree portfast edge default					
2	Portfast enabled on access interface	High	False	False	Matched by equivalent ✓
<b>Comment:</b> Module was marked as matched by equivalent by module 09_01_stp_portfast_default.yaml					
3	BPDU Guard globally enabled	Critical	False	False	Successful ✓
<b>Right configuration setting found in:</b> spanning-tree portfast edge bpduguard default					
4	BPDU Guard enabled on access interface	High	False	False	Matched by equivalent ✓
<b>Comment:</b> Module was marked as matched by equivalent by module 09_03_stp_bpdu_guard.yaml					
5	BPDU Filter globally disabled	Critical	False	False	Successful ✓
6	BPDU Filter disabled on access interface	High	False	False	Not relevant ✓
<b>Comment:</b> Module 09_06_stp_bpdu_filter_interface.yaml configured to run after 09_05_stp_bpdu_filter.yaml with status error but that module has not run yet with specified cmd_match_status, 09_06_stp_bpdu_filter_interface.yaml will not run					
7	Loop Guard globally enabled	Critical	False	False	Successful ✓
<b>Right configuration setting found in:</b> spanning-tree loopguard default					
8	Loop Guard enabled on access interface	High	False	False	Matched by equivalent ✓
<b>Comment:</b> Module was marked as matched by equivalent by module 09_07_stp_loop_guard.yaml					

## VLAN

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Default Vlan not used	Critical	False	False	Error ✗
<b>Comment:</b> Cannot be fixed automatically! Cannot automatically determine VLAN assignment to port.					
<b>Right configuration setting found in:</b> interface Ethernet0/1 switchport access vlan 50 interface Ethernet0/2 switchport access vlan 60					
<b>Found port(s) with error:</b> Ethernet0/3 Ethernet1/0 Ethernet1/1 Ethernet1/2 Ethernet1/3 Ethernet2/0 Ethernet2/1 Ethernet2/2 Ethernet2/3 Ethernet3/0 Ethernet3/1 Ethernet3/2 Ethernet3/3					
<b>Fix notice:</b> Eliminate ports with default Vlan by command with Vlan ID different than 1 interface <interface name> switchport mode access switchport access vlan <vlan id>					

2	Management VLAN + SVI set and different than 1	Medium	False	False	Error ❌
<b>Comment:</b> Cannot be fixed automatically! Cannot automatically set different IP among SVI(s) a lot of prerequisites must be met as existing VLAN and port assigned to VLAN.					
<b>Fix notice:</b> If successful, it means SVI was found, but it might not be management VLAN!! Management VLAN can be created with command: interface Vlan <vlan id> ip address <ip> <mask> no shutdown					
3	Management VLAN gateway	Medium	False	False	Error ❌
<b>Comment:</b> Cannot be fixed automatically! Cannot automatically set default gateway among different switches.					
<b>Fix notice:</b> Default gateway can be set with command: ip default-gateway <ip address>					
4	Native vlan different than 1	Critical	False	False	Successful ✔️
<b>Right configuration setting found in:</b> interface Ethernet0/0 switchport trunk native vlan 100					
5	Specified allowed VLAN on trunk	Critical	False	False	Successful ✔️
<b>Right configuration setting found in:</b> interface Ethernet0/0 switchport trunk allowed vlan 50,60					
6	Switchport mode dynamic disabled	Critical	False	False	Successful ✔️
7	Switchport implicit dynamic disabled	Critical	False	False	Successful ✔️
<b>Right configuration setting found in:</b> interface Ethernet0/1 switchport mode access interface Ethernet0/2 switchport mode access interface Ethernet0/3 switchport mode access interface Ethernet1/0 switchport mode access interface Ethernet1/1 switchport mode access interface Ethernet1/2 switchport mode access interface Ethernet1/3 switchport mode access interface Ethernet2/0 switchport mode access interface Ethernet2/1 switchport mode access interface Ethernet2/2 switchport mode access interface Ethernet2/3 switchport mode access interface Ethernet3/0 switchport mode access interface Ethernet3/1 switchport mode access interface Ethernet3/2 switchport mode access interface Ethernet3/3 switchport mode access					
8	DTP disabled	Critical	False	False	Successful ✔️

**Right configuration setting found in:**

```
interface Ethernet0/0
switchport nonegotiate
interface Ethernet0/1
switchport nonegotiate
interface Ethernet0/2
switchport nonegotiate
interface Ethernet0/3
switchport nonegotiate
interface Ethernet1/0
switchport nonegotiate
interface Ethernet1/1
switchport nonegotiate
interface Ethernet1/2
switchport nonegotiate
interface Ethernet1/3
switchport nonegotiate
interface Ethernet2/0
switchport nonegotiate
interface Ethernet2/1
switchport nonegotiate
interface Ethernet2/2
switchport nonegotiate
interface Ethernet2/3
switchport nonegotiate
interface Ethernet3/0
switchport nonegotiate
interface Ethernet3/1
switchport nonegotiate
interface Ethernet3/2
switchport nonegotiate
interface Ethernet3/3
switchport nonegotiate
```

9	VTP disabled	Critical	False	False	Successful ✓
---	--------------	----------	-------	-------	--------------

## Network Mapping

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	CDP globally disabled	Critical	False	False	Successful ✓
<b>Right configuration setting found in:</b> no cdp run					
2	CDP disabled on interface(s)	Critical	False	False	Matched by equivalent ✓
<b>Comment:</b> Module was marked as matched by equivalent by module 11_01_cdp_run_disabled.yaml					
3	LLDP globally disabled	Critical	False	False	Successful ✓
4	LLDP receive disabled on interface(s)	Critical	False	False	Not relevant ✓
<b>Comment:</b> Module 11_04_lldp_receive.yaml configured to run after 11_03_lldp_run_disabled.yaml with status error but that module has not run yet with specified cmd_match_status, 11_04_lldp_receive.yaml will not run					
5	LLDP transmit disabled on interface(s)	Critical	False	False	Not relevant ✓
<b>Comment:</b> Module 11_05_lldp_transmit.yaml configured to run after 11_03_lldp_run_disabled.yaml with status error but that module has not run yet with specified cmd_match_status, 11_05_lldp_transmit.yaml will not run					
6	ICMP 224.0.0.1 ping disabled in ACL	Medium	False	False	Successful ✓

**Right configuration setting found in:**

```
ip access-list extended DENY_NETWORK_MAP
remark deny ping all nodes
deny icmp any host 224.0.0.1 echo log-input
remark deny host query
deny igmp any any 1 log-input
permit ip any any
remark deny ping all nodes
remark deny host query
```

7	IGMP Host Query disabled in ACL	Medium	False	False	Successful ✓
---	---------------------------------	--------	-------	-------	--------------

**Right configuration setting found in:**

```
ip access-list extended DENY_NETWORK_MAP
remark deny ping all nodes
deny icmp any host 224.0.0.1 echo log-input
remark deny host query
deny igmp any any 1 log-input
permit ip any any
remark deny ping all nodes
remark deny host query
```

8	ICMPv6 ff02::1 ping disabled in ACL	Medium	False	False	Successful ✓
---	-------------------------------------	--------	-------	-------	--------------

**Right configuration setting found in:**

```
ipv6 access-list DENY_NETWORK_MAP_IPV6
remark deny ping all nodes
deny icmp any host FF02::1 echo-request log-input
remark deny mld query
deny icmp any any mld-query log-input
permit ipv6 any any
```

9	MLD Host Query disabled in ACL	Medium	False	False	Successful ✓
---	--------------------------------	--------	-------	-------	--------------

**Right configuration setting found in:**

```
ipv6 access-list DENY_NETWORK_MAP_IPV6
remark deny ping all nodes
deny icmp any host FF02::1 echo-request log-input
remark deny mld query
deny icmp any any mld-query log-input
permit ipv6 any any
```

10	ACL against IPv4 network monitoring applied on interface(s)	Medium	False	False	Successful ✓
----	-------------------------------------------------------------	--------	-------	-------	--------------

**Right configuration setting found in:**

```
interface Ethernet0/1
ip access-group DENY_NETWORK_MAP in
interface Ethernet0/2
ip access-group DENY_NETWORK_MAP in
interface Ethernet0/3
ip access-group DENY_NETWORK_MAP in
interface Ethernet1/0
ip access-group DENY_NETWORK_MAP in
interface Ethernet1/1
ip access-group DENY_NETWORK_MAP in
interface Ethernet1/2
ip access-group DENY_NETWORK_MAP in
interface Ethernet1/3
ip access-group DENY_NETWORK_MAP in
interface Ethernet2/0
ip access-group DENY_NETWORK_MAP in
interface Ethernet2/1
ip access-group DENY_NETWORK_MAP in
interface Ethernet2/2
ip access-group DENY_NETWORK_MAP in
interface Ethernet2/3
ip access-group DENY_NETWORK_MAP in
interface Ethernet3/0
ip access-group DENY_NETWORK_MAP in
interface Ethernet3/1
ip access-group DENY_NETWORK_MAP in
interface Ethernet3/2
ip access-group DENY_NETWORK_MAP in
interface Ethernet3/3
ip access-group DENY_NETWORK_MAP in
```

11	ACL against IPv6 network monitoring applied on interface(s)	Medium	False	False	Error ✗
----	-------------------------------------------------------------	--------	-------	-------	---------

**Found port(s) with error:**

Ethernet0/1  
Ethernet0/2  
Ethernet0/3  
Ethernet1/0  
Ethernet1/1  
Ethernet1/2  
Ethernet1/3  
Ethernet2/0  
Ethernet2/1  
Ethernet2/2  
Ethernet2/3  
Ethernet3/0  
Ethernet3/1  
Ethernet3/2  
Ethernet3/3



**Generated fix:**

```
interface Ethernet0/1
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet0/2
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet0/3
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet1/0
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet1/1
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet1/2
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet1/3
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet2/0
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet2/1
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet2/2
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet2/3
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet3/0
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet3/1
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet3/2
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
interface Ethernet3/3
ipv6 traffic-filter DENY_NETWORK_MAP_IPV6 in
exit
```

**Fix notice:**

ACL will be applied to specified ACCESS interface(s). In case of existing ACL on interface in same direction, please set variable fix\_cmd\_ignore: "true" and append generated ACL from module 11\_14\_icmpv6\_discovery\_network to existing ACL to proper place.

## Filtering

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	ACL filter IPv6 unknown extended header	Critical	False	False	Successful 
<b>Right configuration setting found in:</b> ipv6 access-list IPV6_FRAGMENT_FILTER remark DENY unknown IPv6 extended headers deny ipv6 any any log-input undetermined-transport permit ipv6 any any					
2	ACL filter IPv6 unknown extended header applied on ACCESS interface	Critical	False	False	Error 
<b>Found port(s) with error:</b> Ethernet0/1 Ethernet0/2 Ethernet0/3 Ethernet1/0 Ethernet1/1 Ethernet1/2 Ethernet1/3 Ethernet2/0 Ethernet2/1 Ethernet2/2 Ethernet2/3 Ethernet3/0 Ethernet3/1 Ethernet3/2 Ethernet3/3					
<b>Generated fix:</b> interface Ethernet0/1 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet0/2 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet0/3 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet1/0 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet1/1 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet1/2 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet1/3 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet2/0 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet2/1 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet2/2 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet2/3 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet3/0 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet3/1 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet3/2 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit interface Ethernet3/3 ipv6 traffic-filter IPV6_FRAGMENT_FILTER in exit					

**Fix notice:**

ACL will be applied to specified ACCESS interface. In case of existing ACL on interface in same direction, please set variable fix\_cmd\_ignore: "true" and append generated ACL from module 13\_06\_ipv6\_extended\_header.yaml to existing ACL to proper place.

## First Hop Security

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Port security enabled	Critical	False	False	Successful ✓
<b>Right configuration setting found in:</b> interface Ethernet0/1 switchport port-security interface Ethernet0/2 switchport port-security interface Ethernet0/3 switchport port-security interface Ethernet1/0 switchport port-security interface Ethernet1/1 switchport port-security interface Ethernet1/2 switchport port-security interface Ethernet1/3 switchport port-security interface Ethernet2/0 switchport port-security interface Ethernet2/1 switchport port-security interface Ethernet2/2 switchport port-security interface Ethernet2/3 switchport port-security interface Ethernet3/0 switchport port-security interface Ethernet3/1 switchport port-security interface Ethernet3/2 switchport port-security interface Ethernet3/3 switchport port-security					
2	Port security maximum 1 allowed MAC on port	Critical	False	False	Successful ✓
3	Port security violation shutdown	Critical	False	False	Successful ✓
4	802.1x globally enabled	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> dot1x system-auth-control					
5	AAA authentication 802.1x	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> aaa authentication dot1x default group RADIUS_SERVER					
6	802.1x enabled on interfaces	High	False	False	Successful ✓

**Right configuration setting found in:**

```
interface Ethernet0/1
access-session port-control auto
interface Ethernet0/2
access-session port-control auto
interface Ethernet0/3
access-session port-control auto
interface Ethernet1/0
access-session port-control auto
interface Ethernet1/1
access-session port-control auto
interface Ethernet1/2
access-session port-control auto
interface Ethernet1/3
access-session port-control auto
interface Ethernet2/0
access-session port-control auto
interface Ethernet2/1
access-session port-control auto
interface Ethernet2/2
access-session port-control auto
interface Ethernet2/3
access-session port-control auto
interface Ethernet3/0
access-session port-control auto
interface Ethernet3/1
access-session port-control auto
interface Ethernet3/2
access-session port-control auto
interface Ethernet3/3
access-session port-control auto
```

7	802.1x enabled on interfaces	High	False	False	Successful ✓
8	802.1x port set authenticator	High	False	False	Successful ✓

**Right configuration setting found in:**

```
interface Ethernet0/1
dot1x pae authenticator
interface Ethernet0/2
dot1x pae authenticator
interface Ethernet0/3
dot1x pae authenticator
interface Ethernet1/0
dot1x pae authenticator
interface Ethernet1/1
dot1x pae authenticator
interface Ethernet1/2
dot1x pae authenticator
interface Ethernet1/3
dot1x pae authenticator
interface Ethernet2/0
dot1x pae authenticator
interface Ethernet2/1
dot1x pae authenticator
interface Ethernet2/2
dot1x pae authenticator
interface Ethernet2/3
dot1x pae authenticator
interface Ethernet3/0
dot1x pae authenticator
interface Ethernet3/1
dot1x pae authenticator
interface Ethernet3/2
dot1x pae authenticator
interface Ethernet3/3
dot1x pae authenticator
```

9	DHCP Snooping globally enabled	Critical	False	False	Successful ✓
---	--------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

```
ip dhcp snooping
```

10	DHCP Snooping enabled for VLAN(s)	Critical	False	False	Successful ✓
----	-----------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

```
ip dhcp snooping vlan 10,20,30,40,50,60
```

11	DHCP Snooping trust interface(s) set	Critical	False	False	Successful ✓
----	--------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

```
interface Ethernet0/0
ip dhcp snooping trust
```



12	DHCP Snooping rate limit fo ACCESS interface(s) set	High	False	False	Successful ✓
<b>Right configuration setting found in:</b> interface Ethernet0/1 ip dhcp snooping limit rate 100 interface Ethernet0/2 ip dhcp snooping limit rate 100 interface Ethernet0/3 ip dhcp snooping limit rate 100 interface Ethernet1/0 ip dhcp snooping limit rate 100 interface Ethernet1/1 ip dhcp snooping limit rate 100 interface Ethernet1/2 ip dhcp snooping limit rate 100 interface Ethernet1/3 ip dhcp snooping limit rate 100 interface Ethernet2/0 ip dhcp snooping limit rate 100 interface Ethernet2/1 ip dhcp snooping limit rate 100 interface Ethernet2/2 ip dhcp snooping limit rate 100 interface Ethernet2/3 ip dhcp snooping limit rate 100 interface Ethernet3/0 ip dhcp snooping limit rate 100 interface Ethernet3/1 ip dhcp snooping limit rate 100 interface Ethernet3/2 ip dhcp snooping limit rate 100 interface Ethernet3/3 ip dhcp snooping limit rate 100					
13	IPv6 Unicast Routing enabled	Critical	False	False	Successful ✓
<b>Right configuration setting found in:</b> ipv6 unicast-routing					
14	IPv6 RA Guard host policy defined	Critical	False	False	Successful ✓
<b>Right configuration setting found in:</b> ipv6 nd raguard policy ipv6_raguard_policy					
15	IPv6 RA Guard on ACCESS interface(s)	Critical	False	False	Successful ✓

**Right configuration setting found in:**

interface Ethernet0/1  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet0/2  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet0/3  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet1/0  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet1/1  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet1/2  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet1/3  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet2/0  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet2/1  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet2/2  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet2/3  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet3/0  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet3/1  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet3/2  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy  
interface Ethernet3/3  
ipv6 nd raguard attach-policy ipv6\_raguard\_policy

16	DHCPv6 Server policy	Critical	False	False	Successful ✓
----	----------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

ipv6 dhcp guard policy dhcpv6\_server\_policy  
device-role server

17	DHCPv6 Client policy	Critical	False	False	Successful ✓
----	----------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

ipv6 dhcp guard policy dhcpv6\_client\_policy

18	DHCPv6 Guard server interface(s) set	Critical	False	False	Successful ✓
----	--------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

interface Ethernet0/0  
ipv6 dhcp guard attach-policy dhcpv6\_server\_policy

19	DHCPv6 Guard client interface(s) set	Critical	False	False	Successful ✓
----	--------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

interface Ethernet0/1  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet0/2  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet0/3  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet1/0  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet1/1  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet1/2  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet1/3  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet2/0  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet2/1  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet2/2  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet2/3  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet3/0  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet3/1  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet3/2  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy  
interface Ethernet3/3  
ipv6 dhcp guard attach-policy dhcpv6\_client\_policy

20	Dynamic ARP Inspection enabled for VLAN(s)	Critical	False	False	Successful ✓
----	--------------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

ip arp inspection vlan 10,20,30,40,50,60

21	Dynamic ARP Inspection validate by SRC,DST MAC and IP	Critical	False	False	Successful ✓
----	-------------------------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

ip arp inspection validate src-mac dst-mac ip

22	Dynamic ARP trusted interface(s) set	Critical	False	False	Successful ✓
----	--------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

interface Ethernet0/0  
ip arp inspection trust

23	IPv6 ND inspection policy	Critical	False	False	Successful ✓
----	---------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

ipv6 nd inspection policy ipv6\_nd\_inspection\_policy  
tracking enable

24	IPv6 ND inspection on interface(s) set	Critical	False	False	Successful ✓
----	----------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

```
interface Ethernet0/1
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet0/2
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet0/3
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet1/0
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet1/1
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet1/2
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet1/3
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet2/0
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet2/1
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet2/2
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet2/3
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet3/0
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet3/1
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet3/2
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
interface Ethernet3/3
ipv6 nd inspection attach-policy ipv6_nd_inspection_policy
```

25	IPv6 Snooping policy	Critical	False	False	Successful ✓
----	----------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

```
ipv6 snooping policy ipv6_snooping_policy
security-level glean
```

26	IPv6 Snooping on interface(s) set	Critical	False	False	Successful ✓
----	-----------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

```
interface Ethernet0/0
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet0/1
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet0/2
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet0/3
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet1/0
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet1/1
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet1/2
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet1/3
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet2/0
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet2/1
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet2/2
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet2/3
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet3/0
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet3/1
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet3/2
ipv6 snooping attach-policy ipv6_snooping_policy
interface Ethernet3/3
ipv6 snooping attach-policy ipv6_snooping_policy
```

27	IP Source Guard on interface(s) set	Critical	False	False	Successful ✓
----	-------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

```
interface Ethernet0/1
ip verify source port-security
interface Ethernet0/2
ip verify source port-security
interface Ethernet0/3
ip verify source port-security
interface Ethernet1/0
ip verify source port-security
interface Ethernet1/1
ip verify source port-security
interface Ethernet1/2
ip verify source port-security
interface Ethernet1/3
ip verify source port-security
interface Ethernet2/0
ip verify source port-security
interface Ethernet2/1
ip verify source port-security
interface Ethernet2/2
ip verify source port-security
interface Ethernet2/3
ip verify source port-security
interface Ethernet3/0
ip verify source port-security
interface Ethernet3/1
ip verify source port-security
interface Ethernet3/2
ip verify source port-security
interface Ethernet3/3
ip verify source port-security
```

28	IPv6 Source Guard policy	Critical	False	False	Successful ✓
----	--------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

```
ipv6 source-guard policy ipv6_source_guard_policy
```

29	IPv6 Source Guard on interface(s) set	Critical	False	False	Successful ✓
----	---------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

```
interface Ethernet0/1
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet0/2
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet0/3
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet1/0
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet1/1
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet1/2
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet1/3
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet2/0
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet2/1
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet2/2
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet2/3
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet3/0
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet3/1
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet3/2
ipv6 source-guard attach-policy ipv6_source_guard_policy
interface Ethernet3/3
ipv6 source-guard attach-policy ipv6_source_guard_policy
```












30	IPv6 Destination Guard policy	Critical	False	False	Successful ✓
----	-------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

```
ipv6 destination-guard policy ipv6_destination_guard_policy
```

31	IPv6 Destination Guard on interface(s) set	Critical	False	False	Successful 
<b>Right configuration setting found in:</b> interface Ethernet0/1 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet0/2 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet0/3 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet1/0 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet1/1 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet1/2 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet1/3 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet2/0 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet2/1 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet2/2 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet2/3 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet3/0 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet3/1 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet3/2 ipv6 destination-guard attach-policy ipv6_destination_guard_policy interface Ethernet3/3 ipv6 destination-guard attach-policy ipv6_destination_guard_policy					

## Other

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Servis PAD disabled (Packet assembler disassembler)	High	False	False	Successful 
<b>Right configuration setting found in:</b> no service pad					
2	BOOTP server disabled	High	False	False	Successful 
<b>Right configuration setting found in:</b> no ip bootp server					
3	Finger protocol disabled	High	False	False	Successful 
4	HTTP server disabled	High	False	False	Error 
<b>Error configuration setting found in:</b> ip http server					
5	HTTPS server disabled	High	False	False	Successful 
6	TCP small server disabled	High	False	False	Successful 
7	UDP small server disabled	High	False	False	Successful 
8	IP domain lookup disabled	High	False	False	Successful 
<b>Right configuration setting found in:</b> no ip domain-lookup					
9	Gratuitous ARPs generation disabled	High	False	False	Successful 
<b>Right configuration setting found in:</b> no ip gratuitous-arps					
10	Gratuitous ARPs reject enabled	High	False	False	Successful 
<b>Right configuration setting found in:</b> ip arp gratuitous none					
11	Netflow is disabled	Notice	False	False	Notice 

**Error configuration setting found in:**

ip flow-export destination 192.168.50.11 100

**Fix ignore comment:**

By default fix is ignored due to disablement of traffic monitoring. Consider whether port mirroring is necessary for monitoring

12	Netflow version 9 used	Medium	False	False	Successful ✓
----	------------------------	--------	-------	-------	--------------

**Right configuration setting found in:**

ip flow-export version 9

13	Netflow traffic analyze disabled on interface(s)	Notice	False	False	Notice !
----	--------------------------------------------------	--------	-------	-------	----------

**Error configuration setting found in:**

interface Ethernet0/2

ip flow ingress

**Found ports with error:**

Ethernet0/2

**Generated fix:**

interface Ethernet0/2

no ip flow ingress

interface Ethernet0/2

exit

**Fix ignore comment:**

By default fix is ignored due to disablement of traffic monitoring. Consider whether port mirroring is necessary for monitoring

14	Port mirroring disabled on interface(s)	Notice	False	False	Notice !
----	-----------------------------------------	--------	-------	-------	----------

**Error configuration setting found in:**

monitor session 1 source interface Et0/2

**Fix ignore comment:**

By default fix is ignored due to disablement of traffic monitoring. Consider whether port mirroring is necessary for monitoring

15	Notification on memory IO leak/overflow	Medium	False	False	Error ✗
----	-----------------------------------------	--------	-------	-------	---------

**Generated fix:**

exception memory ignore overflow io

16	Notification on memory CPU leak/overflow	Medium	False	False	Error ✗
----	------------------------------------------	--------	-------	-------	---------

**Generated fix:**

exception memory ignore overflow processor

17	Network boot disabled	Medium	False	False	Successful ✓
----	-----------------------	--------	-------	-------	--------------

18	Network config load disabled	Medium	False	False	Successful ✓
----	------------------------------	--------	-------	-------	--------------

19	SCP server enabled	Medium	False	False	Error ✗
----	--------------------	--------	-------	-------	---------

**Generated fix:**

ip scp server enable

20	SCP alias copy instead of TFTP	High	False	False	Successful ✓
----	--------------------------------	------	-------	-------	--------------

21	Protection of configuration deletion	High	False	False	Error ✗
----	--------------------------------------	------	-------	-------	---------

**Generated fix:**

secure boot config

secure boot-config

**Fix notice:**

Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

22	Archive and log config changes	Medium	False	False	Successful ✓
----	--------------------------------	--------	-------	-------	--------------

**Right configuration setting found in:**

archive  
log config  
logging enable  
notify syslog contenttype plaintext  
hidekeys  
path unix:  
maximum 5  
time-period 60  
memory reserve critical 1000  
memory free low-watermark processor 2000

23	Terminate hanged inbound TCP connection to device	Medium	False	False	Successful ✓
----	---------------------------------------------------	--------	-------	-------	--------------

**Right configuration setting found in:**

service tcp-keepalives-in

24	Terminate hanged outbound TCP connection to device	Medium	False	False	Successful ✓
----	----------------------------------------------------	--------	-------	-------	--------------

**Right configuration setting found in:**

service tcp-keepalives-out

25	Encrypt all saved passwords in configuration	Critical	False	False	Successful ✓
----	----------------------------------------------	----------	-------	-------	--------------

**Right configuration setting found in:**

no service password-encryption